Congress of the United States

Washington, DC 20510

December 19, 2018

The Honorable Kirstjen Nielson
Secretary
U.S. Department of Homeland Security
3801 Nebraska Avenue, NW
Washington, DC 20548

Dear Secretary Nielson:

The U.S. Government Accountability Office (GAO) recently concluded that there are significant weaknesses in the Transportation Security Administration's pipeline security program management.[1] We write today to request the Department of Homeland Security (DHS) perform an assessment of current cyber and physical security protections for U.S. natural gas, oil, and other hazardous liquid pipelines and associated infrastructure. We also request a specific plan of action as to how DHS will address GAO's concerns.

As you know, the Aviation & Transportation Security Act of 2001 created the Transportation Security Administration (TSA), and vested it with authority for pipeline security, including cybersecurity. Pursuant to the "Pipeline Security Guidelines" issued in April 2011, and as updated in March 2018, TSA relies on voluntary guidelines and guidance for the security of our nation's pipeline infrastructure.

The most concerning conclusions of the recently completed GAO review include:

1. TSA does not have a process to update its Pipeline Security Guidelines to ensure consistency with the National Institute for Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity or updates in the cybersecurity space. For much of the guidelines' existence they have not kept pace with the NIST Cybersecurity Framework
2. TSA relies on the industry's self-evaluation using ill-defined criteria provided by TSA to determine whether a specific pipeline operator has a critical facility within its pipeline system. As a result, approximately one third of the top 100 systems based on volume indicated to TSA that they do not have any critical facilities and TSA did not conduct an onsite review of these facilities.
3. TSA has not tracked the status of corporate security review recommendations to pipeline operators for the past five years. As a result, TSA may be unable to determine whether a pipeline operator has corrected any omission or vulnerability identified in a previous site

[1] U.S. Government Accountability Office. *Critical Infrastructure Protection: Actions Needed to Address Significant Weaknesses in TSA's Pipeline Security Program Management,* GAO 19-48. Washington, DC, 2018.

visit. In GAO's words, "[w]ithout current, complete, and accurate information, it is difficult for TSA to evaluate the performance of the pipeline security program." [2]

Addressing our specific questions regarding TSA's guidelines and their effectiveness is needed as a number of major trends have emerged, with potentially significant implications for our energy, national and economic security. These include both the increasing interdependence of U.S. electric and natural gas infrastructure, and the evolving nature of cyber threats from both criminal and foreign state actors.

In 2005, Congress enacted legislation subjecting utilities and others to mandatory reliability, cybersecurity and physical security standards to protect the bulk power system.[3] But, we do not have a similar regime for natural gas pipelines even though natural gas accounts for approximately one-third of all U.S. electric generation. The reliability of the grid is now, more than ever, directly tied to the security of gas pipelines.

Like many grid systems, pipelines are now often operated through Supervisory Control and Data Acquisition (SCADA) systems, which allow greater operational efficiency but are also more vulnerable to cyberattacks. Assessing the cybersecurity posture of our nation's pipeline infrastructure, associated federal policies and partnership efforts is timely and critical. The potential risks are grave, given that an attack on natural gas pipelines could, potentially, cripple the electric grid, which is a significant economic and national security asset.

We ask that DHS provide answers to the following questions:

1. How does the TSA take into account the interdependence of gas pipelines with the electric grid in assessing the "criticality" of the pipeline systems?
2. Many gas pipeline operators have undergone an assessment using the Department of Energy's Cybersecurity Capability Maturity Model. How many pipeline systems in the U.S. have undergone such an assessment? What percentage of industry does this represent? What kind of support is the federal government providing in these assessments?
3. For each year, from Fiscal Year (FY) 2010-FY 2016, how many gas pipeline operators have undergone a TSA inspection and review of their cybersecurity practices? What percentage of gas pipeline operators in the U.S. have undergone such an assessment?
4. Please explain how TSA's program of auditing and inspection follows a risk-based strategy based on criticality of pipeline infrastructure. If the audit and inspection program does not follow a risk-based strategy, what is TSA's criteria for selecting the pipelines that have undergone inspections?
5. What is TSA's selection criteria for cybersecurity standards and metrics used in evaluating gas pipeline operators cybersecurity practices?
6. What percentage of pipeline operators are fully complying with every voluntary cyber security standard of TSA? If you do not have a definite percentage, what is your estimate?

---

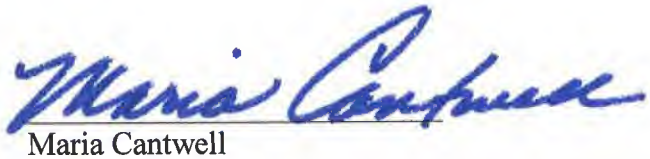
[2] *Id.*
[3] PL 109-58

7. To what extent, if at all, does the Federal Energy Regulatory Commission (FERC) review cybersecurity practices of gas pipeline operators? To what extent does FERC coordinate with TSA on cyber and physical security protections? What policies and procedures, memoranda of understanding, or any other documents govern coordination between FERC and TSA?
8. The Cyber Response Information Sharing Program, piloted by the Department Of Energy (DOE) and its national laboratories, is designed to support the exchange of actionable threat information between government and industry through the Electricity Information Sharing and Analysis Center (E-ISAC), housed at the North American Electric Reliability Corporation (NERC). Does a similar program exist for the oil and gas pipeline sector?
9. How much real time data exchange occurs between the Electricity Information Sharing and Analysis Center, the Oil and Natural Gas Information Sharing and Analysis Center, and the Downstream Natural Gas Information Sharing and Analysis Center? How do these Information Sharing and Analysis Centers support cyber and physical security protections for the oil and gas pipeline sector, and are these efforts effective? Are there technology and structural barriers that prevent the most efficient information sharing? If so, what are they?
10. What are the research and development portfolio priorities of TSA and DHS with respect to pipeline cybersecurity? What is the annual federal expenditure on these activities, and to what extent do these programs leverage private sector investment? To what extent does coordination exist with DOE's Cybersecurity for Energy Delivery Systems?
11. How does DHS work with industry to identify critical infrastructure at greatest risk? How would DHS resolve a potential conflict under Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," specifically sections 6 and 9?
12. If Congress determines that mandatory cybersecurity standards are appropriate for the pipeline industry, which federal entity should enforce those standards?

The results of this assessment will help policymakers evaluate the security of our nation's energy assets, which are critical to the safety, security, and economic well-being of the country. Please provide answers to the above questions, as well as a specific plan of action as to how DHS will address GAO's concerns by no later than January 31, 2019.

Thank you for your consideration.

Sincerely,



Maria Cantwell
Ranking Member, Senate Committee on Energy and Natural Resources

Frank Pallone, Jr.
Ranking Member, House Committee on Energy and Commerce